Reporte: Resultados Primera Consulta Pública sobre Ciberseguridad

Comité Interministerial de Ciberseguridad

PNCS2-D3-20230424

Unidad de Género y Participación Ciudadana
Subsecretaría del Interior

Índice de contenidos

1. Contexto

Nuestro país se encuentra elaborando la Segunda Política Nacional de Ciberseguridad para el período 2023-2028. En el marco de este proceso participativo y abierto, la Coordinación Nacional de Ciberseguridad y la Unidad de Género y Participación Ciudadana de la Subsecretaría del Interior realizaron la Primera Consulta Ciudadana sobre Ciberseguridad, con el propósito de conocer el parecer de la ciudadanía sobre algunas propuestas centrales de lo que será la Política.

Esta minuta presenta los resultados de la consulta. En la sección 2 se presentan las preguntas realizadas, y un breve resumen de las respuestas recibidas. En la sección 3 se caracteriza a las personas que respondieron la consulta; en la sección 4 se presenta la percepción que las personas tienen sobre su conocimiento sobre ciberseguridad, y sobre la importancia que asignan al tema. Finalmente, en la sección 5, aparecen las respuestas a las preguntas principales sobre la Política, y en la sección 6 aparecen las respuestas a las preguntas opcionales.

En todas las secciones que presentan gráficos, se indica la cantidad de personas que respondieron cada pregunta en el mismo gráfico.

2. Preguntas realizadas

La consulta contiene 13 preguntas de selección múltiple, 4 preguntas de caracterización demográfica, y 5 preguntas opcionales, que contenían propuestas de medidas para la Política. Las 5 preguntas opcionales se mostraban sólo si la persona consentía en responderlas (ver la pregunta 18 en la tabla de abajo). La consulta fue comenzada por 1058 personas, y fue terminada por 546 personas (un 51,6%), entre el 3 de marzo de 2023, a las 8:34, y el 10 de abril de 2023 a las 23:44. El tiempo promedio de respuesta fue de 9 minutos y 16 segundos.

En la siguiente tabla se indican las preguntas en el mismo orden en el que fueron realizadas. En la columna de la derecha se indica el código con el que nos referiremos a la pregunta en el análisis posterior, y el tipo de pregunta (principal, demográfica, u opcional).

#	Pregunta	Código y tipo de pregunta
1	Comparado con todas las personas que conoces, ¿cuánto crees que sabes sobre ciberseguridad? Por favor desplaza el círculo abajo con el mouse o tu dedo para indicar tu respuesta.	C1 (principal)
2	¿Cuán importante crees que es la ciberseguridad para el país? Por favor desplaza el círculo abajo con el mouse o tu dedo para indicar tu respuesta.	C2 (principal)
3	¿En qué áreas de tu vida diaria y de tu entorno inmediato crees que el Estado debería proteger más tus datos y tu identidad digital? Marca hasta 3 áreas que creas que son las más importantes. a. Mis finanzas personales, para proteger mi información y mi dinero en bancos e instituciones financieras. b. Mis redes sociales, para protegerme a mí, a mi familia y amigos de engaños. c. Mis redes sociales, para proteger mi emprendimiento o fuente de trabajo. d. Internet, para proteger las organizaciones donde trabajo o estudio de atacantes que pudieran robar y publicar la información. e. Internet, para proteger mi información médica en centros de salud, clínicas y hospitales. f. Internet, para proteger la información de mis compras en tiendas y locales comerciales. g. En mi casa, para proteger mi computador/teléfono/tablet/etc. de virus o de intrusiones de personas externas. h. En los servicios públicos, para proteger la información que los servicios públicos tienen de mí y de mi familia. i. Otra área (¿cuál?)	C3 (principal)
4	La nueva Política Nacional de Ciberseguridad estará organizada en torno a objetivos. Un objetivo es un propósito de alto nivel que queremos lograr como país al 2028.	C4 (principal)

#	Pregunta	Código y tipo de pregunta
	¿Qué importancia le asignas a los objetivos de la Política, indicados abajo? Por favor ordénalos considerando que el de más arriba es el más importante, y el de más abajo es el menos importante. Arrastra cada opción con el mouse o con tu dedo tomando las 3 barras negras a la izquierda. a. Infraestructura resiliente: se refiere a que la infraestructura (es decir, las redes y los aparatos y programas que permiten hacer funcionar las redes) no se "caigan" con facilidad y estén disponibles cuando los necesitamos. b. Protección de derechos de las personas: esta protección debe extenderse para poder proteger el ejercicio de los derechos en Internet. c. Generación de cultura de ciberseguridad: la ciberseguridad es derecho y responsabilidad de todos; cada persona debe tener hábitos básicos de higiene digital, y herramientas para poder protegerse, proteger a su familia, y a las organizaciones en que trabaja o estudia. d. Coordinación nacional e internacional: todas las organizaciones públicas y privadas deben coordinar sus esfuerzos para protegerse y proteger a la sociedad y al resto de las organizaciones del país. e. Fomento a industria de ciberseguridad: los servicios de nuestras empresas en ciberseguridad deben ser promovidos y apoyados, y deben estar disponibles para personas y organizaciones de nuestro país.	
5	La infraestructura crítica de información de un país son todos aquellos servicios que posibilitan el funcionamiento de aquella infraestructura que, de no estar disponible, podría afectar gravemente el bienestar o la salud de las personas en el país. Por ejemplo, un hospital no puede funcionar sin energía eléctrica, y las empresas de distribución de energía eléctrica no pueden funcionar sin Internet. La conexión a Internet es entonces parte de la infraestructura crítica del país. En tu opinión, ¿cómo debería ser protegida la infraestructura crítica de información del país? Marca un máximo de 3 opciones que consideres aplicables. a. Las organizaciones de infraestructura crítica deberían ser protegidas físicamente por las Fuerzas Armadas. b. La autoridad debería exigir a las organizaciones de infraestructura crítica normas más estrictas que al resto de las	C5 (principal)

#	Pregunta	Código y tipo de pregunta
	empresas, para que en caso de catástrofe, las redes se mantengan en funcionamiento. c. Las organizaciones de infraestructura crítica deberían ser auditadas regularmente por una Agencia de Gobierno independiente. d. Las organizaciones de infraestructura crítica deberían ser auditadas regularmente por empresas de seguridad informática para que cumplan con los estándares de certificación internacional. e. Las organizaciones de infraestructura crítica deberían reportar al menos una vez al año el nivel de protección que otorgan a sus instalaciones, y la cantidad y tipo de ataques que han recibido durante el año. f. Otra medida (¿cuál?)	
6	La nueva Política Nacional de Ciberseguridad incluirá algunos temas transversales. Estos son temas a los que daremos especial importancia. En tu opinión, ¿qué tan importante es incluir el siguiente tema transversal en la nueva Política? "Enfoque de Género y Paridad: todas las iniciativas deben considerar de manera transversal la perspectiva de género y la paridad, entendida como la participación equilibrada entre hombres y mujeres para avanzar hacia la igualdad sustantiva." [Las alternativas para esta pregunta son una escala tipo Likert de 5 puntos: “Es muy importante”, “Es importante”, “Tiene la misma importancia que otros temas”, “Es poco importante”, “No es importante”]	C6 (principal)
7	En tu opinión, ¿qué tan importante es incluir el siguiente tema transversal en la nueva Política Nacional de Ciberseguridad? "Protección a la niñez: todas las iniciativas deben considerar protección preferente a niñas, niños y adolescentes." [Las alternativas para esta pregunta son una escala tipo Likert de 5 puntos: “Es muy importante”, “Es importante”, “Tiene la misma importancia que otros temas”, “Es poco importante”, “No es importante”]	C6 (principal)
8	En tu opinión, ¿qué tan importante es incluir el siguiente tema transversal en la nueva Política Nacional de Ciberseguridad?	C6 (principal)

#	Pregunta	Código y tipo de pregunta
	"Protección al adulto mayor: todas las iniciativas deben considerar protección preferente a adultos mayores." [Las alternativas para esta pregunta son una escala tipo Likert de 5 puntos: “Es muy importante”, “Es importante”, “Tiene la misma importancia que otros temas”, “Es poco importante”, “No es importante”]	
9	En tu opinión, ¿qué tan importante es incluir el siguiente tema transversal en la nueva Política Nacional de Ciberseguridad? "Protección del medioambiente: todas las iniciativas deben minimizar su impacto negativo sobre el medio ambiente." [Las alternativas para esta pregunta son una escala tipo Likert de 5 puntos: “Es muy importante”, “Es importante”, “Tiene la misma importancia que otros temas”, “Es poco importante”, “No es importante”]	C6 (principal)
10	En tu opinión, ¿qué tan importante es incluir el siguiente tema transversal en la nueva Política Nacional de Ciberseguridad? "Descentralización del territorio: todas las iniciativas deben apuntar a descentralizar la toma de decisiones, y equiparar los recursos a los que tienen acceso las distintas zonas del país." [Las alternativas para esta pregunta son una escala tipo Likert de 5 puntos: “Es muy importante”, “Es importante”, “Tiene la misma importancia que otros temas”, “Es poco importante”, “No es importante”]	C6 (principal)
11	En tu opinión, ¿qué tan importante es incluir el siguiente tema transversal en la nueva Política Nacional de Ciberseguridad? "Protección de la vida privada: todas las iniciativas deben proteger la privacidad de las personas y su autodeterminación para decidir cuánto de su vida privada deciden compartir públicamente." [Las alternativas para esta pregunta son una escala tipo Likert de 5 puntos: “Es muy importante”, “Es importante”, “Tiene la misma importancia que otros temas”, “Es poco importante”, “No es importante”]	C6 (principal)

#	Pregunta	Código y tipo de pregunta
12	En tu opinión, ¿qué tan importante es incluir el siguiente tema transversal en la nueva Política Nacional de Ciberseguridad? "Protección a personas en situación de discapacidad: todas las iniciativas deben considerar la protección a personas que, en relación a sus condiciones de salud física, psíquica, intelectual, sensorial u otras, al interactuar con diversas barreras contextuales, actitudinales y ambientales, presentan restricciones en su participación plena y activa en la sociedad." [Las alternativas para esta pregunta son una escala tipo Likert de 5 puntos: “Es muy importante”, “Es importante”, “Tiene la misma importancia que otros temas”, “Es poco importante”, “No es importante”]	C6 (principal)
13	La industria de ciberseguridad es el conjunto de empresas que ofrecen servicios relacionados con la protección de los datos de personas y organizaciones. En Chile existe un conjunto acotado de empresas que ofrecen estos servicios. ¿Crees que existen barreras para el desarrollo de la industria de ciberseguridad? a. No, no creo que existan barreras b. No lo sé, no estoy seguro(a) c. Sí, creo que existen barreras [Esta pregunta incluyó un campo de comentarios abiertos.]	C7 (principal)
14	¿Cuál es tu edad? [Campo de texto simple]	D1 (demográfica)
15	¿Cuál es tu género? a. Femenino b. Masculino c. No binario d. Prefiero no responder	D2 (demográfica)
16	¿En qué comuna vives? [Se incluyó una lista con todas las comunas.]	D3 (demográfica)
17	¿Cuál es el máximo nivel educacional que terminaste? a. Educación básica	D4 (demográfica)

#	Pregunta	Código y tipo de pregunta
	b. Educación media c. Educación técnica superior (centro de formación técnica) d. Educación profesional o universitaria (en institutos profesionales o universidades) e. Educación terciaria (magíster o doctorado) f. Ninguna de las anteriores	
18	Muchas gracias por responder esta consulta ciudadana. Tus respuestas serán analizadas y utilizadas para generar la nueva Política Nacional de Ciberseguridad. Tenemos 5 preguntas adicionales que nos ayudarán a decidir sobre las medidas a implementar en la nueva Política. ¿Quieres responder estas preguntas adicionales? a. Sí, quiero responder ahora b. No, no quiero responder más preguntas	Pregunta auxiliar, sin código
19	En la siguiente pregunta encontrarás una serie de medidas que podrían ser incluidas o no dentro de la nueva política, en el objetivo "Infraestructura resiliente". Por favor escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Infraestructura resiliente". a. Rediseño y actualización de la Ley General de Telecomunicaciones, para crear incentivos de mercado para garantizar que todas las comunas de Chile estén conectadas, y que esta conexión sea robusta. b. Definir trazados de fibra óptica necesarios para conectar todas las comunas que aún no se encuentran conectadas, y ver la factibilidad de licitar la conexión de estas comunas. c. Diseñar un servicio de monitoreo y medición de calidad de servicio de acceso a Internet en Chile. Esto permitiría al país enterarse cuando un lugar ha quedado sin conexión, para poder recuperar la conexión de forma rápida. d. Encargar a una o más universidades un estudio de la red lógica (ruteo IP) sobre las redes existentes de fibra óptica, para determinar estrategias automáticas de reconexión en caso de desastres, como terremotos o tsunamis que dejan lugares sin conexión. e. Otra medida (¿cuál?) f. No tengo suficiente información para responder esta pregunta.	M1 (opcional)

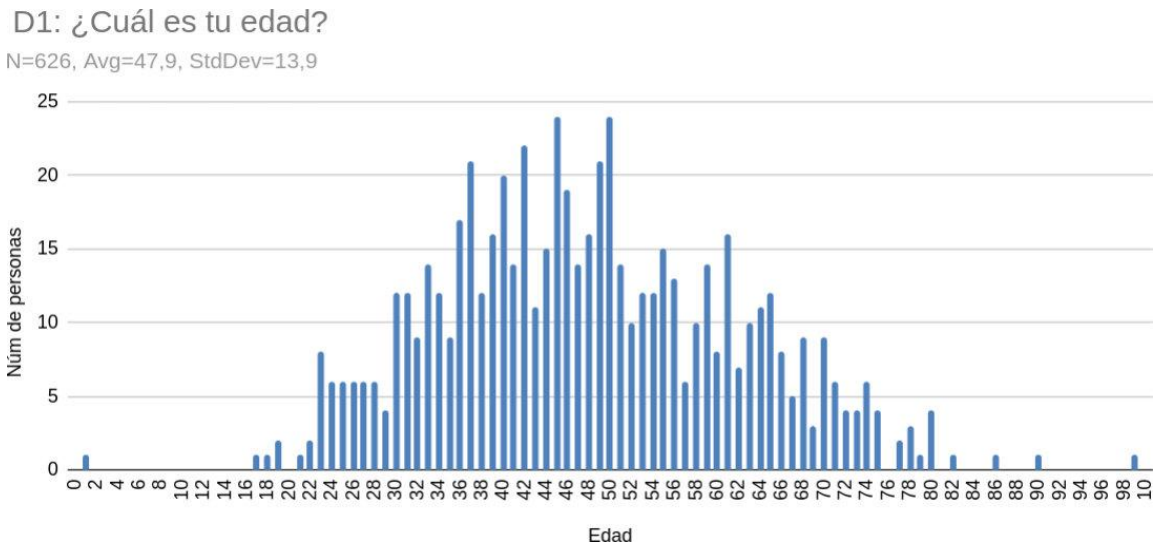
#	Pregunta	Código y tipo de pregunta
20	En la siguiente pregunta encontrarás una serie de medidas que podrían ser incluidas o no dentro de la nueva política, en el objetivo "Derechos de las personas". Por favor escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Derechos de las personas". a. Creación de un sitio web centralizado para la denuncia de estafas y suplantaciones en Internet; este sitio web sería como una ventanilla única de denuncia de delitos, que conectaría directamente a las policías y el ministerio público. b. Creación de cursos básicos, gratuitos y en línea, para público en general, sobre el derecho a la privacidad en Internet, y sobre cómo usar cifrado para los mensajes personales (que sirve para proteger la privacidad de las personas). c. Generación de campañas de protección contra el stalkerware (apps maliciosas de espionaje a través del smartphone; se usa típicamente por hombres para controlar a sus parejas). d. Encargar a una o más universidades un estudio para saber qué tan frecuentemente se dan casos de discriminación de datos en la red por parte de proveedores de servicios de Internet (lo que se conoce como "neutralidad de la red"). e. Otra medida (¿cuál?) f. No tengo suficiente información para responder esta pregunta.	M2 (opcional)
21	En la siguiente pregunta encontrarás una serie de medidas que podrían ser incluidas o no dentro de la nueva política, en el objetivo "Cultura de ciberseguridad". Por favor escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Cultura de ciberseguridad". a. Creación de un plan de concientización nacional sobre ciberseguridad y privacidad, para que todas las personas adquieran nociones de higiene digital, a través de municipalidades y organizaciones civiles. b. Agregar higiene digital y nociones de ciberseguridad a los planes curriculares de la educación general básica y media, para que todos los niños y niñas sepan cómo cuidar su información y protegerse en Internet.	M3 (opcional)

#	Pregunta	Código y tipo de pregunta
	c. Creación de cursos básicos, gratuitos y en línea sobre cómo proteger la información y la identidad propia en Internet para público en general, con especial foco en adultos mayores. d. Creación de carreras técnicas en la enseñanza media técnico-profesional sobre ciberseguridad. e. Otra medida (¿cuál?) f. No tengo suficiente información para responder esta pregunta.	
22	En la siguiente pregunta encontrarás una serie de medidas que podrían ser incluidas o no dentro de la nueva política, en el objetivo "Coordinación nacional e internacional". Por favor escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Coordinación nacional e internacional". a. Establecer instancias de cooperación con países avanzados en materia de respuesta de incidentes, como Estonia, Estados Unidos, Reino Unido y Países Bajos; y ser anfitrión de eventos internacionales de ciberseguridad con invitados de estos países. b. Fortalecer el Centro de Respuesta a Incidentes Informáticos de la Subsecretaría del Interior, para que se transforme en un centro nacional de respuesta a incidentes. c. Crear centros de investigación y transferencia tecnológica público-privados en ciberseguridad, donde se investiguen temas de interés para el país. d. Impulsar programas de financiamiento o becas para profesionales técnicos en otros países más avanzados en ciberseguridad. e. Otra medida (¿cuál?) f. No tengo suficiente información para responder esta pregunta.	M4 (opcional)
23	En la siguiente pregunta encontrarás una serie de medidas que podrían ser incluidas o no dentro de la nueva política, en el objetivo "Fomento a industria de ciberseguridad". Por favor escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Fomento a la industria de ciberseguridad". a. Generar incentivos para la creación de emprendimientos tecnológicos en ciberseguridad.	M5 (opcional)

#	Pregunta	Código y tipo de pregunta
	b. Crear incentivos tributarios y económicos para la instalación de empresas internacionales de ciberseguridad en Chile, en áreas que sean de especial interés para el país. c. Promocionar los productos y servicios de las empresas locales en ciberseguridad en el extranjero, a través de fondos públicos. d. Crear o fortalecer instrumentos de fomento a la internacionalización de empresas locales de ciberseguridad. e. Otra medida (¿cuál?) f. No tengo suficiente información para responder esta pregunta.	

3. Caracterización demográfica

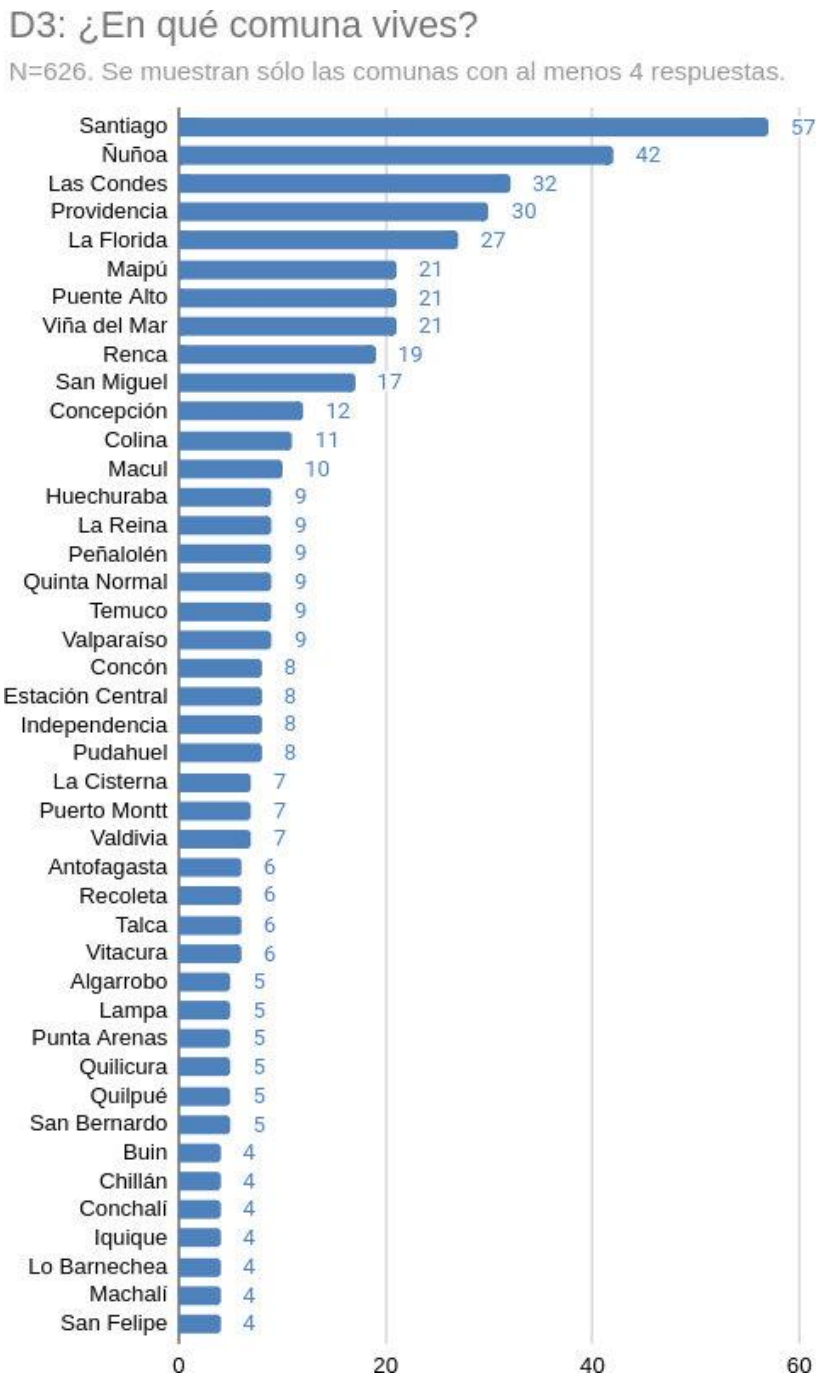
El siguiente gráfico muestra la distribución de edades declaradas por los respondentes. El promedio de edad es de 47,9 años, con una desviación estándar de 13,9 años.



En el siguiente gráfico se muestra el género declarado por las personas que respondieron la pregunta. Un 37,2% respondieron “Femenino”, un 59,7% respondieron

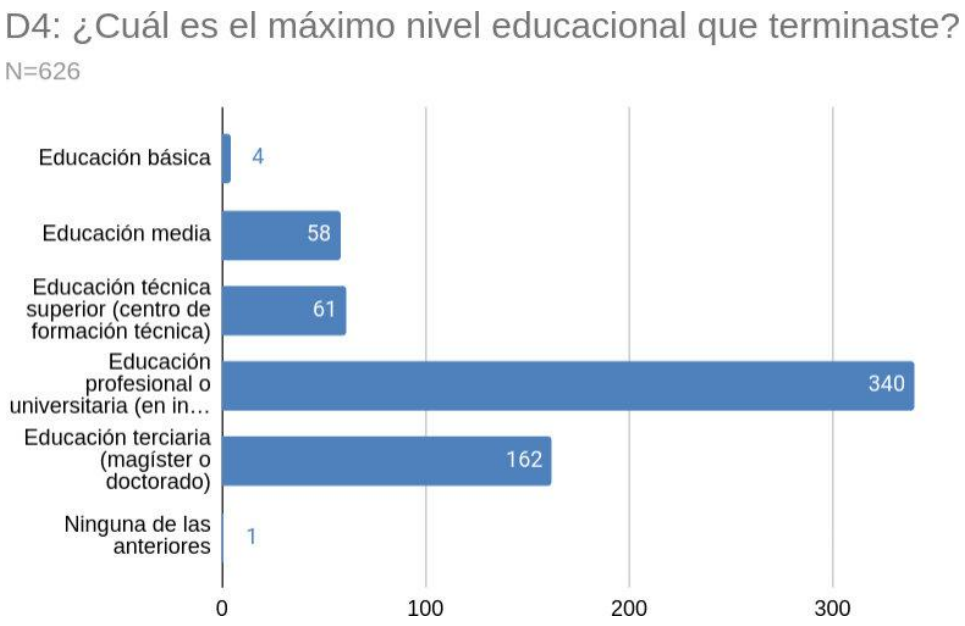
"Masculino", 4 personas (un 0,6%) respondieron "No binario", y 15 personas (un 2,4%) escogieron la opción "Prefiero no responder".

En el siguiente gráfico se muestran las respuestas a la pregunta "¿En qué comuna vives?". Se muestran sólo las comunas con 4 respuestas o más. En el anexo 1 se muestra el resto de las comunas y la cantidad de respuestas que recibieron. Dos tercios de las respuestas (408, un 65,2%) provienen de comunas en la Región Metropolitana.



En el siguiente gráfico se muestra el máximo nivel educacional de las personas que respondieron la pregunta. Un 54,3% tiene educación universitaria, un 25,9% tiene

formación de postgrado (magíster o doctorado), un 9,7% tienen educación técnica superior, un 9,3% tienen educación media, y un 0,6% declara tener educación básica.



En síntesis, hablamos de una población de edad promedio 48 años, con una mayoría de hombres, predominantemente de la zona central del país, con un alto capital cultural, y en su mayoría probablemente de un nivel económico medio a alto.

4. Percepción sobre ciberseguridad

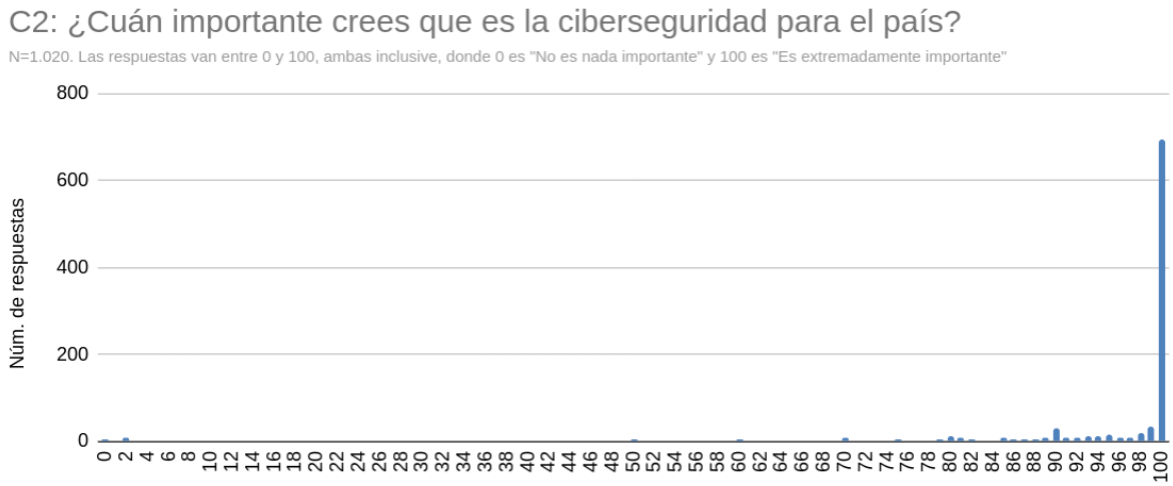
La pregunta 1 fue diseñada para entender qué percepción de conocimiento tiene la persona sobre ciberseguridad. La respuesta fue a través de un control que podía arrastrarse, y que podía moverse hacia la izquierda o a la derecha. En el extremo izquierdo pusimos el texto “Todos saben más que yo”, y en el extremo derecho pusimos el texto “Yo sé más que todos los demás”. Dado que esta pregunta es relativa al círculo cercano de la persona que responde, y que la respuesta es un número entre 0 y 100, en esta pregunta debería observarse una distribución normal. La pregunta 2 fue diseñada para entender cuál es el nivel de importancia que la persona atribuye al tema ciberseguridad.

A pesar de que estas no son preguntas demográficas, fueron incluidas para caracterizar de mejor forma a las personas que respondieron la encuesta.

En el gráfico siguiente se observa la distribución de las respuestas a la pregunta C1.

Se observa que, salvo por el extremo derecho, se puede observar una distribución que podría corresponder a una normal muy aplastada, con promedio aproximadamente igual a 50 y una gran desviación estándar. Sin embargo, hubo más de 150 respuestas (alrededor del 14%) que respondieron con el extremo derecho; es decir, alrededor del 14% de las personas que responden se consideran expertas en ciberseguridad.

En el siguiente gráfico se observan las respuestas a la pregunta C2.



La mayor parte de las personas (alrededor de 700 o 70%) creen que la ciberseguridad es extremadamente importante para el país.

5. Preguntas principales

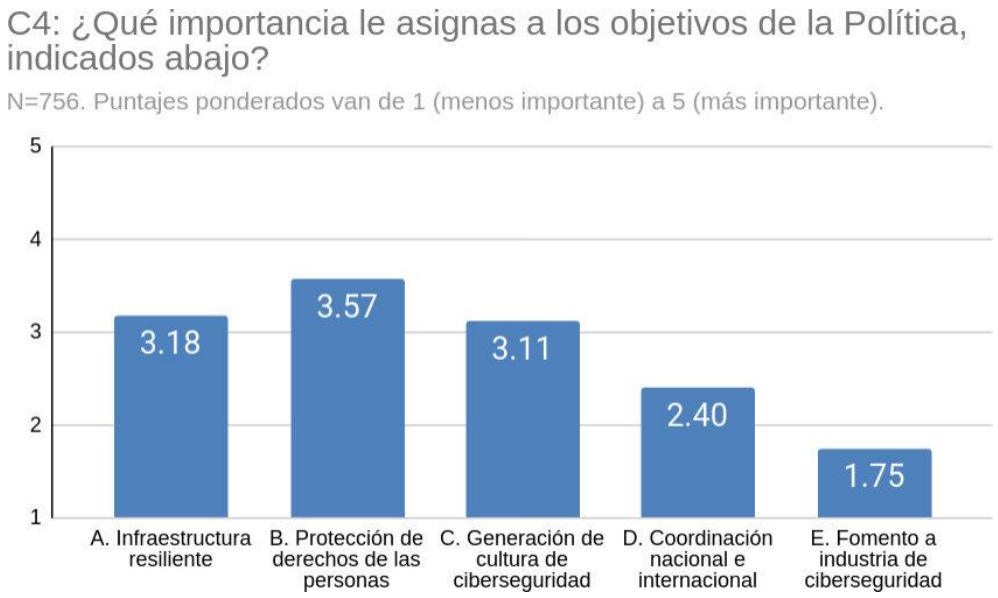
En el siguiente gráfico, se observan las respuestas a la pregunta C3. Las alternativas a esta pregunta fueron presentadas aleatoriamente a cada persona; por tanto, no debiera haber un sesgo de orden en la selección de alternativas en esta pregunta.

En el gráfico anterior, es relativamente claro que las dos áreas en que se considera que el Estado debería intervenir más para proteger los datos e identidad de las personas es en los mismos servicios públicos, y en las instituciones financieras.

En esta pregunta, se dio a las personas la opción de proponer otras áreas con la alternativa “Otra área (¿cuál?)”. Las respuestas adicionales se presentan sin editar y

ordenadas alfabéticamente en el anexo 2 (sólo se filtró una respuesta con texto ininteligible).

En el gráfico siguiente, se observa la importancia relativa que las personas que respondieron la consulta le otorgan a los objetivos centrales propuestos para la nueva Política, que son una modificación de los objetivos incluidos en la primera Política.



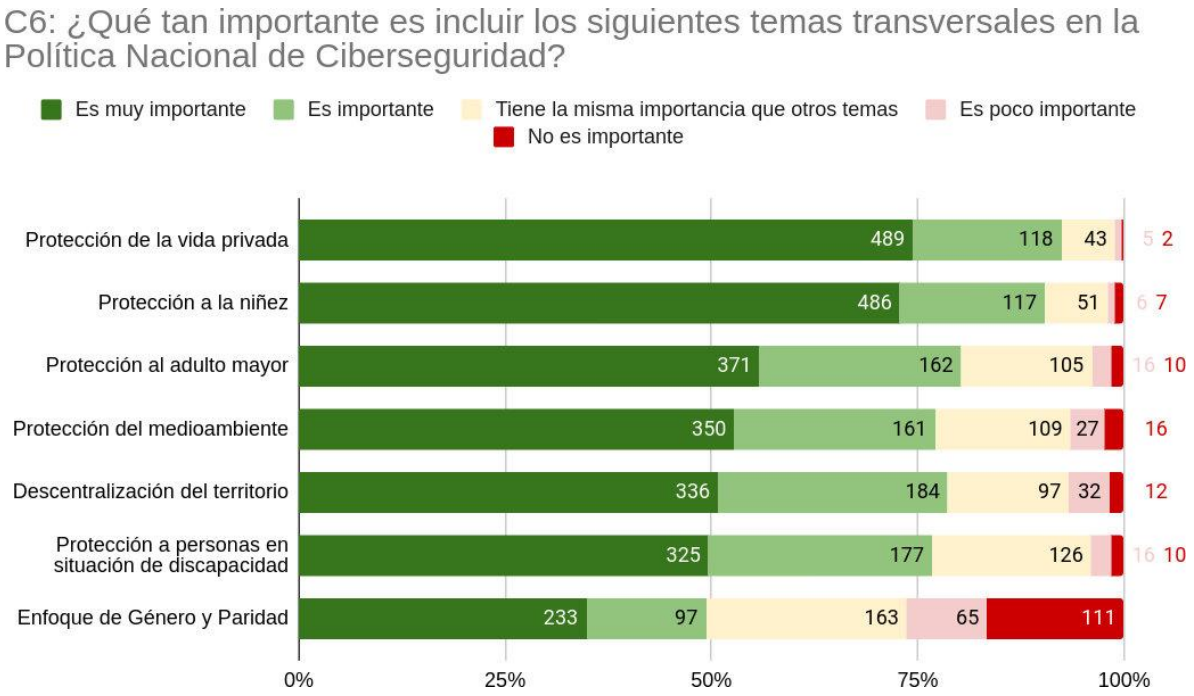
El siguiente gráfico muestra las respuestas a la pregunta C5, ordenadas por número de votos. Las alternativas a esta pregunta fueron presentadas aleatoriamente a cada persona; por tanto, no existe en esta pregunta un sesgo de orden en la selección de alternativas.

C5: ¿Cómo debería ser protegida la infraestructura crítica de información del país?

N=686. Se podía marcar hasta 3 opciones.

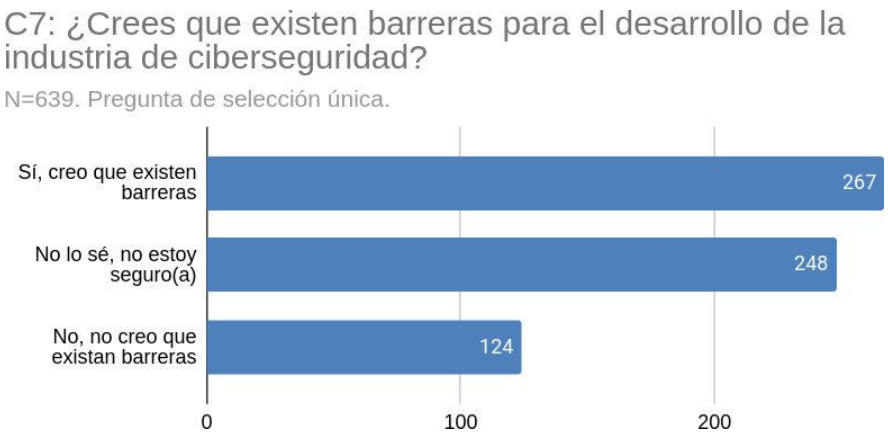
En la pregunta anterior se ofreció la posibilidad de sugerir otras formas en las que debería ser protegida la infraestructura crítica. En el anexo 3 se presentan estas respuestas.

En el gráfico siguiente se observa la percepción de importancia que las personas que respondieron la consulta otorgaron a diversos temas propuestos a ser incluidos en la nueva Política, ordenados en orden descendente.



En términos relativos, los dos temas considerados más importantes fueron la protección a la vida privada y la protección a la niñez. Por contraposición, los dos temas con menos percepción de importancia fueron la protección a personas en situación de discapacidad y un enfoque de género y paridad.

En el gráfico siguiente se observan las respuestas a la pregunta C7, sobre industria de ciberseguridad.



6. Preguntas opcionales

En los gráficos a continuación se observan las respuestas a las preguntas con código M1 a M5. En todas las preguntas las alternativas fueron presentadas aleatoriamente a cada persona; por tanto, no debiera haber un sesgo de orden en la selección de alternativas. Las alternativas están ordenadas en orden decreciente de número de preferencias. Debajo del título se presenta el número de personas que respondió cada pregunta.

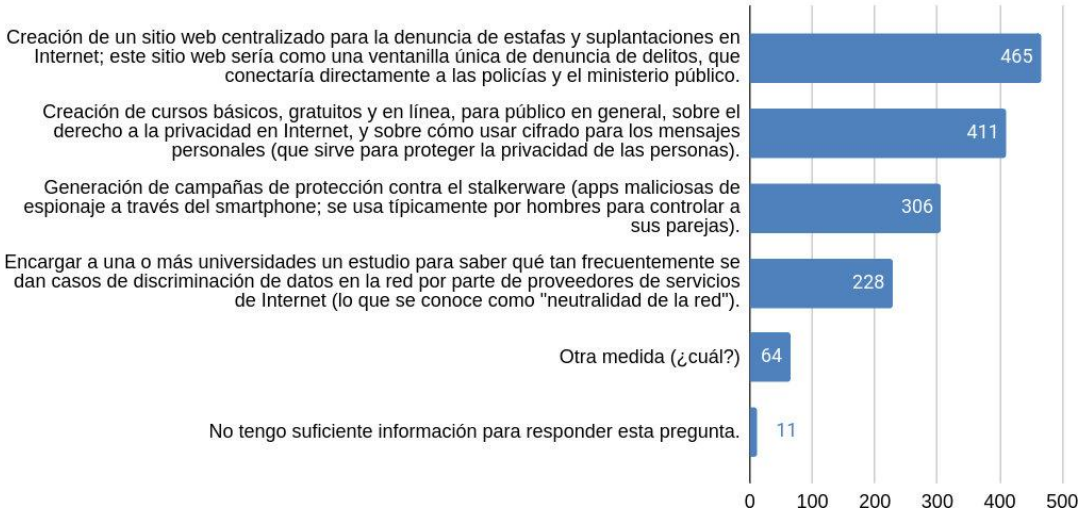
En el gráfico a continuación se presentan las medidas más votadas en el objetivo "Infraestructura resiliente":

58 personas propusieron medidas adicionales o hicieron comentarios a la pregunta anterior. En el anexo 4 se presentan estos textos, sin editar ni filtrar y ordenados alfabéticamente.

En el gráfico a continuación se presentan las medidas más votadas en el objetivo "Derechos de las personas":

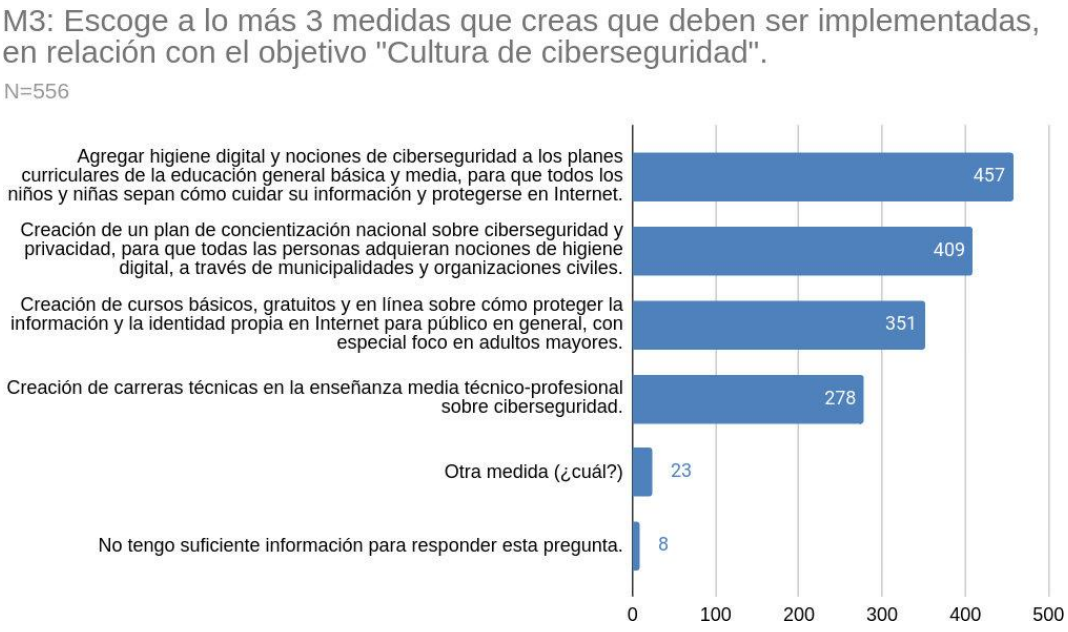
M2: Escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Derechos de las personas".

N=562



64 personas propusieron medidas adicionales o hicieron comentarios a la pregunta anterior. En el anexo 5 se presentan estos textos, sin editar ni filtrar y ordenados alfabéticamente.

En el gráfico a continuación se presentan las medidas más votadas en el objetivo “Cultura de ciberseguridad”:

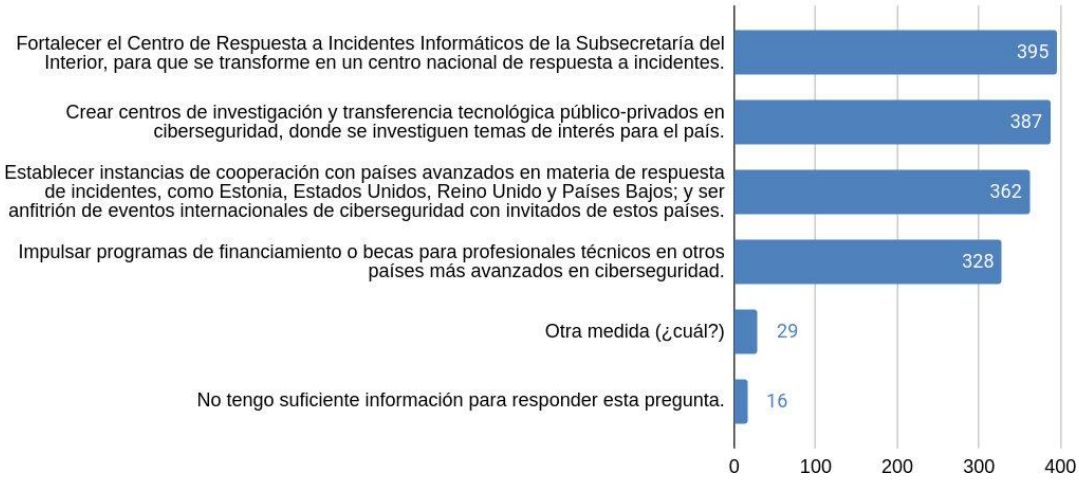


23 personas propusieron medidas adicionales o hicieron comentarios a la pregunta anterior. En el anexo 6 se presentan estos textos, sin editar ni filtrar y ordenados alfabéticamente.

En el gráfico a continuación se presentan las medidas más votadas en el objetivo “Coordinación nacional e internacional”:

M4: Escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Coordinación nacional e internacional".

N=553



29 personas propusieron medidas adicionales o hicieron comentarios a la pregunta anterior. En el anexo 7 se presentan estos textos, sin editar ni filtrar y ordenados alfabéticamente.

Finalmente, en el gráfico a continuación se presentan las medidas más votadas en el objetivo “Fomento a la industria de ciberseguridad”:

42 personas propusieron medidas adicionales o hicieron comentarios a la pregunta anterior. En el anexo 8 se presentan estos textos, sin editar ni filtrar y ordenados alfabéticamente.

Anexo 1: Respuestas desde otras comunas

Desde cada una de las siguientes comunas se recibieron 3 respuestas: Cabo de Hornos, Cerrillos, Cerro Navia, Copiapó, Coquimbo, Curicó, El Bosque, Hualpén, Linares, y Rancagua.

Desde cada una de las siguientes comunas se recibieron 2 respuestas: Angol, Calera de Tango, Cochrane, Curacaví, La Serena, Limache, Los Ángeles, Los Vilos, Melipilla, Molina, Osorno, Paine, Pedro Aguirre Cerda, Peñaflor, Peumo, Pirque, San Fernando, San Pedro de La Paz, San Ramón y Villarrica.

Desde cada una de las siguientes comunas se recibió sólo 1 respuesta: Alto Hospicio, Andacollo, Arica, Cabrero, Calama, Caldera, Castro, Cauquenes, Chépica, Chiguayante, Chillán Viejo, Codegua, Colbún, Coronel, El Tabo, Graneros, Juan Fernández, La Calera, La Cruz, La Granja, La Pintana, Lo Espejo, Lo Prado, Los Álamos, Lumaco, Marchihue, Maule, Natales, O'Higgins, Olmué, Padre Hurtado, Parral, Pelarco, Pica, Pinto, Pitrufquén, Pozo Almonte, Quellón, Quillota, San José de Maipo, Talagante, Talcahuano, Teno, Tucapel, Vallenar, Vilcún y Villa Alemana.

Anexo 2: Respuestas adicionales en la pregunta C3

La pregunta C3 fue: "*¿En qué áreas de tu vida diaria y de tu entorno inmediato crees que el Estado debería proteger más tus datos y tu identidad digital?*" Las personas podían escoger a lo más 3 dentro de un conjunto de opciones, y podían proponer áreas adicionales. En la siguiente lista se presentan las áreas propuestas por las personas que respondieron la pregunta.

Las siguientes respuestas se presentan **sin editar** y ordenadas alfabéticamente (sólo se omitió una respuesta con texto ininteligible).

1. A mi como ciber persona las compañías prestadoras de servicio se desentienden cuando ya instalan el servicio de internet en los hogares y no implementan mejores medidas de ciber seguridad para las personas
2. Aquellas areas no cubiertas por las protecciones o seguros que las areas privadas poseen
3. Áreas relacionadas con la educación, colegios, institutos, universidades, entre otras.
4. Casa comerciales. No existe privacidad todos los comercios manejan nuestra información.
5. Circulación de información falsa en las redes sociales espcíficamente durante los procesos electorales

6. Crear oficina del estado que vele por la seguridad informática en donde la ciudadanía pueda quejarse y con poder sancionador sobre aquellas entidades que vulneren la seguridad en Internet

7. Creo que el foco debe ser el objetivo de la información. Por ejemplo si una persona cae en urgencias el doctor debiera tener acceso al historial médico. O si una persona postula a un subsidio del Estado que sus cuentas bancarias levanten el secreto bancario para evitar aprovechamientos indebidos o fraudes.

8. Cualquier área estatal donde se manejen datos personales, pues son confidenciales

9. Cybersecurity supply chain risk management

10. Datos básicos personales que se usan en las bases de datos

11. Debería disponer de equipos de expertos que puedan respaldar y asesorar a las pequeñas empresas

12. Debiera protegernos del Estado mismo.

13. Debieran sacar una ley que nos proteja en todas las áreas y que se cumpla

14. Defensa nacional

15. Defensa nacional e infraestructura crítica

16. El Estado debería prestar especial atención a la protección de los datos y la identidad digital en áreas como la salud, las finanzas, la educación y las comunicaciones en línea, y establecer medidas de seguridad adecuadas para garantizar la privacidad y protección de los datos personales de los ciudadanos.

17. En el ámbito de la seguridad personal para prevenir extorsiones y que personas con fines delictuales puedan cometer sus actos

18. En el manejo y almacenamiento de los datos personales y en la venta de los mismos

19. En el sector privado, para que mejoren sus estándares de protección de datos

20. En general instituciones que llaman y ofrecen productos/servicios sin autorización

21. En general redes sociales ..publicaciones de comercios ilícitos de drogas y ventas de vehículos sin papeles

22. En la Información de geolocalización, de dónde estoy, mis rutas, mis direcciones y desplazamientos.

23. En los partidos Políticos para proteger las opiniones io es en confianza

24. En mi casa para protege mis aparatos tecnicos de virus y de los jakes

25. En todas

26. En todas las anteriores. Se requiere una política que aborde los diferentes ámbitos del quehacer digital, tanto de las aplicaciones como la infraestructura que la sustente. Todas las entidades del Estado y empresas deben contar con niveles de ciberseguridad que reduzcan los riesgos para el sistema. De igual forma, los usuarios deben tener una conducta digital responsable.

27. En todo, sobre todo en aquellas páginas del mismo gobierno

28. Energia

29. Es importante establecer un plan de ciberseguridad a nivel escolar, si entregamos buena educación cívica y ciberseguridad en los colegios ello va capitalizar en las futuras y nuevas generaciones.

30. Escuelas e instituciones que trabajan con menores de edad, para Proteger sus datos e información personal y familiar

31. Fraude por internet

32. Incrementar el nivel de seguridad de los servicios de identidad digital que el Estado le proporciona a los ciudadanos, en particular el servicio: ClaveUnica. En otros países se manejan diferentes niveles de acceso según el tipo de trámite que la persona quiere realizar. Ej. SPID en Italia, puede tener hasta 3 niveles diferentes de acceso, accionables a través de más factores de autenticación (no sólo una clave). Acceder a trámites no demasiado críticos o sensibles basta un acceso de Nivel 1 (un solo factor de autenticación), acceder a cosas más sensibles (ej. datos sanitarios de la persona) requiere un Nivel 2 como mínimo (dos factores de autenticación), etc.

33. Infraestructura Crítica (entornos OT) e Infraestructura Crítica de la Información

34. Infraestructura critica de energía

35. Infraestructura crítica.

36. Infraestructura crítica.

37. Infraestructuras criticas, energía, agua, hospitales, municipios, banca, etc...

38. Ingeniería social, noticias falsas, sugestion comercial y política en base a beneficios de algunos por sobre el bien común.

39. Internet, para proteger la información personal de los oligopolios multinacionales que viven de nuestros datos (Microsoft, Alphabet , Meta, Amazon, Apple, Bytedance y más)

40. Internet, para proteger mis datos personales de comercios que hacen mal uso de mi información, como por ejemplo, la venta de datos no autorizados

41. Limitar tik tok, es impresionante cómo la delincuencia narcotraficantes muestran su armamento, "cantantes" urbanos mostrando armas CREAR UNA LEY

42. Más que tener un rol activo en la protección de los datos, debe generar marcos normativos y aplicar regulaciones sobre estos datos, ya sea de los datos almacenados por empresas de Telecomunicaciones, Farmacias, Aseguradoras, Financieras/Bancarias, etc. El "compartir" los datos de los chilenos debería ser fuertemente regulado y obligar a las empresas el saber "qué datos" tiene de cada uno aparte del "dónde" tiene cada uno de esos datos almacenados.

43. Mi rut, toda vez que uso carne y código QR

44. Normativas sobre privacidad de datos y derecho al olvido. Transparencia en la forma en que las empresas e instituciones trabajan y resguardan los datos

45. Para proteger a las personas de las difamaciones en redes sociales donde nadie se hace responsable.

46. Poner límites, reglas, y regulaciones a los permisos que privados pueden acceder.

47. Preocúpense de que no los hackeen y de los audios de la cancilleria y sus ministros y de dar el 10 por ciento que prometieron de lo contrario vayanse

48. Protegerse los niños , de las redes venta y engaño a niños niñas pedofilios que se disfrazan de personas que no son verdaderos para engañar

49. QUÉ EL COMERCIO Y EMPRESAS NO ENTREGUEN LA INFORMACION CONFIADA A OPERADORES EXTERNOS Y DE OTROS PAISES.

50. Redes sociales

51. Regular la custodia y transferencia de datos personales privados

52. Salud publica

53. Salud, electricidad, telecomunicaciones en especial sistemas de emergencia como sae, sistema penal, jurídico y legislativo

54. Se debería considerar inclusive la creación de una identidad digital única, los datos tienen más valor que el oro, las empresas viven del procesamiento de los datos, pero no se regula el uso y creación de decisiones en base a la información de millones de usuarios, millones de datos, es tan complejo que podríamos estar hace años ante la destrucción de la democracia, a partir de datos se pueden cambiar las tendencias de una elección política en un país. Es muy importante considerar regular o permitir el control, uso y mal uso de los datos de todos los chilenos, quizás considerar la authorization y access a partir de una base descentralizada sobre la tecnología block chain, que no sea Google, MS y Amazon los custodios de los datos, por el contrario el usuario debe ser el único dueño de sus datos y él debe decidir cuando, como y con quién compartirlos. Pero ninguna institución privada debería tener resguardo de mis datos.

55. Seguridad Nacional

56. Toda área debería ser protegida, tanto en lo personal, laboral y de terceros, cualquiera no debería obtener información de otros, sino ser solicitada ante el ente competente

57. Todas

58. Una ley efectiva contra el spam telefónico que es cada día más insoportable

Anexo 3: Respuestas adicionales en la pregunta C5

La pregunta C5 tenía una breve introducción para explicar qué es infraestructura crítica. Luego, continuaba así: "*En tu opinión, ¿cómo debería ser protegida la infraestructura crítica de información del país?*" Las personas podían escoger a lo más 3 dentro de un conjunto de opciones, y podían proponer medidas de protección adicionales. En la siguiente lista se presentan las medidas propuestas por las personas que respondieron la pregunta.

Las siguientes respuestas se presentan **sin editar** y ordenadas alfabéticamente (se filtró una respuesta con texto no inteligible):

1. Contar con profesionales del mejor nivel tanto en las areas de gestion como de operaciomes de seguridad, junto con presupuestos no sujetos a la discrecionalidad de la DIPRES

2. Control desde el estado

3. CSIRT Sectoriales para compartir información relevante

4. Deben ser responsables de la mantención del servicio de manera preventiva y redundante

5. Debería pasar a administración privada para que por fin hayan incentivos de hacer las cosas bien

6. Debería tener ética de trabajo y responsabilidad con el resto del entorno

7. Deberian exigir planes de continuidad del negocio que sean probados y acordé a su actividad económica

8. Definir una normativa basada tanto en las condiciones locales como en la experiencia internacional

9. desarrollar industria nacional estatal de energía y telecomunicaciones, que nos permita tener autonomía de las empresas de turno que nos proveen de estos servicios

10. El gobierno debe exigirle la transparencia de la seguridad y que paguen ese trabajó inadecuado con penas efectivas no como el yerno de Pinochett y más encima se quedó con las riquezas de chile (el litio)

11. El poder de la justicia debería tener atribuciones para castigar y sancionar delitos de tráfico de información falsa y sancionar a las redes sociales que permiten la circulación y promueven el odio, el negacionismo y violan los derechos humanos

12. El robo de fibra óptica ya es un problema que afecta a todos

13. Exigir a las telc9 monitoreo de seguridad en servicios hogar

14. Generar instancias de coordinación efectiva entre todos los entes involucrados con la ciberseguridad

15. Infraestructura crítica quedó superado en EU, nuevo concepto: Operadores de Servicios Esenciales (OSE)

16. La autoridad debe regular y definir normas y estándares que deben tener las infraestructura critica.

17. La información del país no puede depender solo de una infraestructura o de 1, 2 o 3 proveedores de nube, se debe pensar en mayor tecnológia y privacidad, los datos son oro para una nación hay que evitar que privados, y estados ajenos al nuestro estén capturando y logrando identificar tendencias sin que los usuarios sepan como se usa o mal usan los datos, es cosa de transparencia, se debe poder como mínimo tener un sistema de tracking de mis datos (algo minimo es poder saber que privado utiliza mi run, mi nombre, mi apellido, correo entre otros para cualquier actividad) Un estado debe garantizar que los datos de los chilenos no serán mal utilizados por ejemplo para afectar la democracia.

18. la infraestructura critica en estos casos debe ir aparejada del entendimiento de los usuarios sobre el uso de las plataformas, los ciberataques, etc.

19. La infraestructura TI debería estar 100% en la nube

20. La pregunta está mal enfocada. El contexto indica que sin internet no funciona la empresa eléctrica, por lo tanto, la empresa eléctrica debiese tener un enlace de respaldo para tener internet siempre. La pregunta está enfocada en la protección de la información, la cual está alojada en un Data Center. El cual ya cumple con las medidas de seguridad suficientes para poder realizar sus funciones.

21. Las empresas con infrestructura crítica deben tener Directores independientes expertos en ciberseguridad que permitan monitorear y supervisar al management en los temas de ciberseguridad

22. Las OIC deben recibir fuertes sanciones en caso de incumplimiento de las normas de seguridad.

23. Las organizaciones de estructura critica deberian contar con los mejores profesionales

24. Las organizaciones de infraestructura crítica deben tener un marco regulatorio y de control externo y experto que los audite regularmente.

25. Las organizaciones de infraestructura crítica deberían estar obligados por el Estado a tener auditorías constantes, de empresas confiables o del mismo estado en alguna organizacion, pero además tener una auditoría o certificación (parecida a la de acreditación de las universidades).

26. Nacionalizar las redes de infraestructura crítica de información.

27. NERC-CIP

28. No inventen organismos/agencias que consumen recursos con ignorantes mayoritariamente. Fomenten leyes que persigan eficazmente los delitos y protejan la infraestructura critica con los instrumentos actuales, mas que suficiente.
29. Otorgar protección al cún de los ciudadanos a precios más módicos
30. Participar de programas de inversión e implemtanción de plataformas de vanguardia para homologar su resiliencia
31. Regular el reporte de incidentes en tiempo y forma. Multar y atribuir responsabilidades a los ejecutivos
32. Reportar todo incidente que afecte el normal funcionamiento, según modelos de criticidad
33. Revisión de la sociedad civil
34. Tener estándar de contratación, capacitación para los funcionarios de seguridad.
35. Tener un servicio que "verifique" experimentalmente y regularmente el nivel de seguridad de la infraestructura crítica
36. Toda la Infra critica debe estar en manos del Estado

Anexo 4: Respuestas adicionales en la pregunta M1

La pregunta M1, así como las que siguen, presentaba una serie de medidas propuestas, que podrían ser incluidas en la Política, en un objetivo central específico. El texto de la pregunta fue el siguiente: "*Por favor escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Infraestructura resiliente"*." La pregunta incluyó un comentario abierto donde las personas podían proponer nuevas medidas; la lista a continuación detalla las medidas propuestas por las personas.

Las siguientes respuestas se presentan **sin editar** ni filtrar y ordenadas alfabéticamente:

1. 1. Introducir redes de comunicaciones REDUNDANTES (no solo las más baratas). 2. Por favor revisar la definición y medidas ref. "Operadores de Servicios Esenciales (OSE)" de ENISA.

2. Actualmente, los proveedores de servicios de Internet (ISP) tienen la capacidad de monitorear la calidad del servicio que brindan, identificando las áreas donde la conexión no está funcionando correctamente y aquellas donde se está funcionando de manera óptima. Sin embargo, la información obtenida a partir de este monitoreo no siempre es transmitida de manera transparente al cliente, lo que puede generar reclamos y problemas de gestión dentro de la industria privada. Las empresas proveedoras de servicios ofrecen una serie de compromisos, como acuerdos de nivel de servicio (SLAs) y medición de tiempo de actividad (uptime), ya que las interrupciones en la comunicación pueden generar pérdidas millonarias para sectores como los bancos. A pesar de esto, los consumidores no siempre cuentan con las mismas garantías y, sin embargo, pagan por los servicios con su dinero. Por lo tanto, para mejorar la relación entre los clientes y los proveedores de servicios de Internet, es fundamental que exista una mayor transparencia en la información sobre la calidad del servicio. De esta manera, los clientes podrán tomar decisiones informadas sobre qué proveedores de servicios elegir y, en caso de surgir algún problema, podrán resolverlo de manera más eficiente y sin la necesidad de realizar reclamos en línea o por teléfono. Para lograr esto, es necesario que los ISP implementen una infraestructura resiliente que les permita monitorear y comunicar con claridad la calidad del servicio a sus clientes en tiempo real.

3. Al igual que el roaming nacional, los ISP puedan en forma conjunta asegurar la conexión de los usuarios al verse afectos por interrupción y/o cortes de enlaces

4. Ampliar cobertura a zonas rurales (no solo con fibra) o zonas mas alejadas. Donde las personas se sienten mas desconectadas. Si bien la fibra es un medio barato la combinación de tecnologías y medios es la mejor respuesta a un sistema robusto

5. Aparato o Agencia del Estado que proteja a la ciudadanía cuando sean dañadas, lesionadas ante las empresas, bancos, etc por cyberataques o fraudes cibernéticos

6. Apoyo a las municipalidades para implementar medidas de acceso Internet en cada comuna

7. Asegurar espacios "oscuros" (No conectados) para no exponer culturas; crear instancia de I+D nacional

8. Aun cuando la universalización de la conectividad es necesaria para el desarrollo digital, no es condición para tener una política de ciberseguridad y procesos / procedimientos / conductas seguras

9. Bajar costos para el consumidor

10. Cableado subterráneo, como los delincuentes son ignorantes se roban la fibra, dejando a los hogares sin internet.

11. Cambiar/ampliar servidores banco estado. Minvu

12. con el fin de tener autonomía energética ante desastres y siempre, se podrían instalar paneles solares en techos de todos los hospitales, SAR, SAMU, recintos policiales, militares y bomberos, y readecuar su instalación eléctrica.

13. Contar con una Empresa Nacional de Telecomunicaciones, para que no todas las opciones como ocurre en esta pregunta estén relacionadas a generar incentivos en el mercado o ver posibilidades de factibilidad para licitar.

14. Creación de un CSIRT de Infraestructuras críticas

15. CSIRT Sectoriales que apoyen la contención y recuperación

16. Debería exigir que las empresas extranjeras que están lucrando con chile entreguen esas erramientas a las universidades y que el estado no les siga llenando de dólares los bolsillos

17. Definir planes de resilencia frente a ataques para infraestructura crítica de electricidad, agua y otras industrias críticas

18. Definir trazados seguros, protegidos y con rutas alternativas de fibra óptica, sin perder la contigencia satelital.

19. Delincuencia en robo de cables fibra debe considerarse como un delito que afecta infra critica

20. Disponer de una arquitectura resiliente acoplada a la infraestuctura a traves de comunicación de emergencia para uso por ejemplo en desastres naturales

21. El Estado debe asegurar autonomía funcional en el resguardo y preservación de los datos independiente de que esa tarea esté delegada en un proveedor externo. Si el proveedor es atacado o pierde los datos la repartición pública debe ser capaz de funcionar de manera soberana y autónoma.

22. El rediseño y actualización de la Ley General de Telecomunicaciones debe velar porque no sigan existiendo "sectores rojos", sectores de la población donde actualmente las compañías no llevan Fibra óptica y obligan prácticamente al ciudadano a utilizar una o dos compañías disponibles (Entel y VTR generalmente porque siguen trabajando con cable, creando monopolios).

23. El sistema de monitoreo debería obtenerse automáticamente del monitoreo mandatado en la ley de velocidad mínima de internet, que aunque no es muy útil al menos podría servir para eso.

24. Estatizar la industria de ciberseguridad y de internet, o al menos menos asegurarse de ser un socio mayoritario en la industria, ya que es un sector estratégico que debe estar al servicio del proyecto país, no implica gratuidad de servicio sino que asegurar que el costo sea justo y que los beneficia se dirijan al desarrollo país

25. Evaluar otros mecanismo de comunicaciones como una red satelital de Internet (alianzas) o que las fuerzas armadas tengan redes paralelas en caso de desastre sirvan de respaldo.

26. Expropiar empresas existentes para formar una empresa nacional de telecomunicaciones.

27. Fiscalización el género de telecomunicaciones

28. Generar estudios y aplicación en instituciones de infraestructura crítica de normas de ciberseguridad cómo ISO 27001, nist 800

29. Icentivar/Fomentar/Obligar el uso de IPv6 domiciliario, utilización de IPSEC y fomentar o crear Puntos de Intercambio de Trafico (PIT) en donde todos los proveedores compartan trafico.

30. Impulsar incentivos a tecnologías inhalambricas como soporte a la infraestructura resiliente (BWS)

31. Incorporar a los profesionales de Ciberseguridad en una instancia público privada para la discusión de iniciativas y elaboración de medidas hacia un sistema nacional de protección.

32. Internet gratis en comunas pobres

33. Internet publica en áreas y espacios de uso público.

34. Internet satelital tipo starlink

35. Inventario y levantamiento de todos los sitios críticos tanto estatales como privados, establecer condiciones residentes de operación, efectuar auditorias e inspecciones permanentes y monitoreo aleatorio on line de su operación en condiciones borde. Parecido a lo que se hizo después del 27F pero ahora al amparo de una ley. Además se debe exigir a las reparticiones públicas que den servicios de atención a la comunidad que cuenten con al menos un experto en infraestructura crítica que se haga

responsable de mantener y probar esta infraestructura, sin prejuicio de la responsabilidad administrativa del jefe de la repartición. La agencia del estado encargada de verificar este cumplimiento debe ser autónoma y aspecializada.

36. Inversión Estatal, no se puede dejar algo tan relevante en manos de privados a través de "incentivos de mercado"

37. La infraestructura resiliente requiere de conexiones redundantes sobre diferentes medios (fibra óptica, cobre, inalámbrica, etc)

38. Las redes deben funcionar con un esquema mesh no con un pto a pto como pasa en muchos sectores de Chile

39. licitar la conectividad reuniendo paquetes de comunas, de tal forma que quien se lo adjudique deba entregar conectividad a comunas pobladas y económicamente sustentable y otras comunas que no sean rentables.

40. Mayor inversión en investigacion y desarrollo orientado a fortalecer la seguridad de la información en el país

41. Me gustaria internet gratuito para los estudiantes y personas mayores los grandes abandonados en este país llamado Chile.

42. Multas a los proveedores de servicio, cuando dicho servicio se suspende por que el proveedor no ha tomado los resguardos del caso

43. no desperdicien tiempo ni hagan gastar fondos inutilmente a las empresas que saben lo que hacen, el desconocimiento disfrazado de agencia estatal solo retrasa la toma efectiva de medidas. Los incentivos y el diseño resiliente de servicios basicos es la clave, no sacan nada con monitorear algo que no entienden.

44. No mas censura de parte del estado ni hackers

45. Organismo estatal independiente que controle el cumplimiento de las normas

46. Potencial redes inalámbricas

47. protección militar de la infraestructura de internet

48. Proveer un enlace de respaldo satelital para las instituciones criticas, Ministerios, Hospitales, FFAA, entre otras.

49. Que las compañías funcionen en alta disponibilidad entre ellas

50. red de transporte dwdm nacional agnostica a los isp

51. Resilencia satelital para catástrofes
52. respecto a la pregunta una universidad, existen mas instituciones que tambien pueden realizar un mismo estudio, analisis y recomendaciones sin desmedro a una universidad
53. Respetar exigencias técnicas de instalación, la altura y el enjambre de cables.
54. Se debe generar e impulsar una segunda red paralela troncal, por una ruta distinta a la actual, que permita brindar continuidad de servicios en caso de eventos naturales o de fuerza mayor que impliquen caídas del servicio primario. EJ: Podría ser para aquellas zonas de dificil acceso, o que cuenten con una única ruta de acceso, contemplar servicios satelitales como servicios de respaldo o secundarios.
55. ser selectivo, basar las inversiones en un análisis integral y desarrollar planes de contingencia para los casos en los que no se justifica aumentar la resiliencia.
56. Transformación digital del estado
57. VPN en Defensa, Ministerio Interior, Ministerio de Hacienda, Ministerio Economía, Ministerio Relaciones Exteriores y toda la Infraestructura Crítica incluyendo empresas Adquirentes como Transbank o Telnet
58. Wi-Fi gratis

Anexo 5: Respuestas adicionales en la pregunta M2

La pregunta M2 presentaba una serie de medidas propuestas, que podrían ser incluidas en la Política, en un objetivo central específico. El texto de la pregunta fue el siguiente: "*Por favor escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Derechos de las personas"*." La pregunta incluyó un comentario abierto donde las personas podían proponer nuevas medidas; la lista a continuación detalla las medidas propuestas por las personas.

Las siguientes respuestas se presentan **sin editar** ni filtrar y ordenadas alfabéticamente:

1. Actualizar la ley 19628 sobre protección de la vida privada, para que equiparase a otras regulaciones internacionales como GDPR, LGPD o CCPA.

2. Adaptar la legislación a las necesidades actuales y futuras de la protección de la información de las personas manejadas por terceros.

3. Adoptar la GDPR y con ella, requerir que toda organización que tenga tráfico internet en el país la cumpla. La neutralidad en la red, es necesario medirla periodicamente. Regular la captura y uso de datos desde proveedores, por ejemplo el trafico DNS y consultas web de las personas.

4. Campañas de co cientizacion permanentes

5. Campañas informativas sobre los derechos enfocado principalmente en el manejo de los datos personales

6. Campañas televisadas de los cursos a implementar, motivando a la población desde jóvenes a empezar su carrera.

7. Capacitación presencial sobre alfabetización digital y uso de redes sociales

8. Castigar severamente acciones de cibercrimen

9. Cómo protegerse cuando el Estado decide en el Derecho de las Personas

10. Creación de una unidad especialista de pdi con comunicación con entidades financieras que pueda congelar fondos en caso de denuncia de robo de fondos financieros de forma electrónica o identificación de fondos financieros relacionado a delitos informáticos cómo cobro de dinero de criptolocker

11. Creación del instituto nacional de ciberseguridad

12. Crear un equipo altamente capacitado de gente especializada en Ciberseguridad, no solo temas del estado como lo es el CSIRT, sino un departemento de CIberDefensa Nacional, en donde existan personas especialistas en defensa, en ataque, en inteligencia, no como la basura de la ANI "un ente pasado a política, capas de mentir según el gobierno de turno o el color político del director", sino un ente que se preocupe por el país independiente del Gobierno de turno.

13. Crear una superintendencia sobre protección de los datos personales y el derecho a la conexión

14. Crearía un sistema de control ciudadano, no necesariamente en tiempo real, para acceder a las acciones intrusivas del estado de manera de poder supervigilar que las

policías están usando correctamente la herramientas NECESARIAS para combatir el cibercrimen

15. Curso obligatorio en el colegio

16. Cursos avanzados para los encargados de redes de los servicios y Ministerios.

17. cursos de ciberseguridad basicos para phishing y buenas practicas

18. Dar facultades al estado para fiscalizar y sansionar el mal uso de datos e información

19. deben hacer campañas que lleguen a toda la sociedad por distintos medios de comuniación, los cursos por internet solo serían realizados por aquellos que tienen buena conexión

20. Debiera existir un ente que viera todos los temas de seguridad del estado y fiscalizará toda entidad de gobierno, uniformar criterios SO, software etc. que este entregue las directrices de las versiones y compras

21. Disminuir el aparato público

22. Educacion desde la educacion pre escolar sobr estrategias de conocimiento/defensa digital

23. Enseñar a los niños a usar redes sociales y navegar en la red, ya que ellos son los principales usuarios y benefactores que nos entrega la web.

24. Enseñar a todos los grupos etarios como detectar un phishing, vishing, smishing, etc. Y que las telcos asuman su responsabilidad en la suplantación.

25. Enseñar ciberseguridad desde el liceo

26. Exigir el derecho de saber cuándo un cliente está en empresa afectados de ransomware oportunamente

27. Fomentar un cultura país proactivamente, cursos no sirven

28. Fortalecer el derecho penal con sanciones concretas ante violaciones a los derechos de las personas.

29. Fortalecer ley protección de datos personales, crear una agencia nacional de protección de datos, desarrollo de funciones relacionadas con la protección de la información

30. Generación de campañas de educación digital contra el phishing, spear phishing, Bloatware, etc. con especial atención a los adultos mayores y personas con mas dificultad para el aprendizaje digital

31. Generar leyes de compensación cuando las empresas públicas fallen en su protección de datos que obligatoriamente piden a los ciudadanos

32. generar medida ejemplificadora ya sea multas o trabajo social cuando sean mal empleados las redes sociales por ejemplos funas

33. Generar un ente fiscalizador con capacidad legal para denunciar el mal uso de la información privada de empresas

34. Generar y financiar iniciativas para promover conductas sanas en las redes sociales

35. Herramientas simples de denuncia y capacitación de las personas, para estar informado y que sea una opción poder denunciar

36. Implementar desde el colegio talleres orientados al uso y riesgos de Internet y redes sociales, respecto de difusión de información personal

37. Incentivar a empresas privadas de comunicaciones, para que realicen campañas sobre seguridad a sus clientes

38. Incluir ramos de ciberseguridad en los colegios de enseñanza básica y media.

39. Incorporar en planea de estudio en colegios esta tematica

40. Incremento de persecucion del tráfico de datos personales en internet

41. Inversión estatal en I+D del tema; asegurar el derecho a la no conexión

42. La implementación de la Ley de Transformación Digital contempla la interoperabilidad como el intercambio de datos con persistencia (o copia) de los datos de una institución a otra, ese es un riesgo innecesario porque la institución consumidora podría perder los datos o se pederá la trazabilidad de uso de los mismos. La solución debe ir por el lado de que los datos solo estén en la fuente primaria original y existan mecanismo para autoriozar la vista de ellos por un tiempo definido que asegure trazabilidad del uso por parte de funcionarios y otras personas.

43. La opción de un estudio de neutralidad de la red le corresponde a subtel, no a una política de ciberseguridad.

44. Las personas debe poseer acceso libre y soberano a las configuraciones de seguridad de los servicios que su ISP contratado le proporciona

45. Las propuestas no van al centro de lo que es la generación de una política de ciberseguridad robusta.

46. Le educación vecinal creo que les están quedando muchos chilenos debajo del puente producti de la ineficientes de los programas tecnológicos que sólo a favorecido en este minuto a los extranjeros que están llegando mucho más avanzados que los chilenos analicen la tecnología está muy al deve en Chile y al gobierno le importa un.... espero lo tome en cuenta

47. los mismo que la anterior abrir los espacios no solo a universidades

48. Mejorar la ley de protección de datos personales

49. Potestad de los ciudadanos de que si información o datos sean borrados cuando lo solicite a cualquier privado

50. Promover la importancia de utilizar applicaciones o servicios que aseguren la privacidad, seguridad, y la propiedad de los datos

51. Publicidad orientadora y educadora sobre el tema

52. Que las denuncias y otras formas de fiscalización sean parte del quehacer del Gobietno Local, como parte de su rol Garante principal de Derechos

53. Que tengamos el derecho a proteger nuestra dignidad ante las calumnias en entornos digitales, pudiendo recibir apoyo desde las instituciones al vernos vulnerados, de manera ágil

54. Realizar una consulta pública que diagnostique el estado actual de alfabetización digital a lo largo del país PREVIO a ejecutar cualquier otra medida. Sin ese estado del arte, es difícil diseñar políticas públicas efectivas.

55. Reformas legales para la prevención y combate de la violencia de género digital más allá del ámbito penal

56. regular y transparentar el traspaso y venta de datos personales entre empresas y terceros

57. Respecto a stalkerware y otros usos malicionsos, incorporar a los operadores en el filtrado, preveción y educación de los usuarios.

58. Revisar la ley europea de protección de datos de usuarios y replicar lo aplicable

59. Sacar el proyecto de ley urgente de Protección de Datos personales que a tardado mucho en el Senado

60. se usa típicamente por hombres pésima redacción victimista. Lo usa gente enferma, punto.

61. Sitio que permita denunciar uso indebido de la información o incuplimiento de sus políticas. Existe mucho software que filtra información confidencial y no cumplen con estándares internacionales

62. un desglose de las campañas de protección: entendido con el uso extendido de APP para comercio, refuerzo de las implicancias del uso de cada uno de ello, promoción de doble autenticación y sus fundamentos, restringir el uso de RUT para la fidelización en comercios.

63. Un sitio web centralizado que permita exigir respuestas a grandes empresas de internet, como Google y Facebook

64. Una especie de superintendencia de ISP y BD que monitoree, regule y fiscalice las empresas y organismos de estado en que transite, procese o almacene la data de personas y grupos de empresa o estado.

Anexo 6: Respuestas adicionales en la pregunta M3

La pregunta M3 presentaba una serie de medidas propuestas, que podrían ser incluidas en la Política, en un objetivo central específico. El texto de la pregunta fue el siguiente: "*Por favor escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Cultura de ciberseguridad"*." La pregunta incluyó un comentario abierto donde las personas podían proponer nuevas medidas; la lista a continuación detalla las medidas propuestas por las personas.

Las siguientes respuestas se presentan **sin editar** ni filtrar y ordenadas alfabéticamente:

1. Agregaría asignaturas de comportamiento básico en la sociedad, entre ellos ciberseguridad, formación financiera, formación legal, etica, etc.

2. Apoyo a instituciones de base en estos temas

3. Creación de las Olimpiadas Escolares de Ciberseguridad para fomentar la ciberseguridad en sus diferentes dimenciones

4. Creaciòn de subsecretaría de ciberseguridad

5. Crear una organización de voluntarios que asistan adultos mayores. Los cursos gratuitos no tienen mucha posibilidad de ser exitosos porque los adultos mayores tienen demandas más complejas en cuanto a ciberseguridad.

6. Cursos para niños, pero no asociados al plan de educación, depende de la familia si lo toma o no.

7. Dar apoyo a los que trabajamos en ciberseguridad para dar o dictar charlas en colegios y universidades.

8. Educacion y difusion desde temprana edad, es la medida mas eficaz para crear cultura.

9. Exigencia a las empresas proveedoras de servicio Internet para el control y filtros a sitios maliciosos

10. Fomento de campos laborales en los que puedan insertarse quienes cursen las carreras técnicas de la alternativa 1; no es eficiente educar para luego no poder hacer uso de esas capacidades en favor de las personas.

11. Fondos sociales concursables de ciberseguridad

12. Laboratorios enfocados en distintas edades con énfasis en la protección en ciberseguridad

13. Las campañas deben realizarse de manera periodica, de la misma forma que en las organizaciones se requiere para cumplir con estandres como ISO27001. El foco puede ir cambiando entre adultos mayores, redes sociales, compras en linea, phishing, etc.

14. Las carreras técnicas y profesionales, el punto es que la ciber seguridad se debe abordar a nivel general de todas las personas, técnicas y profesionales

15. Legislar

16. Limitar el acceso a Juegos On line a menores de 14 años

17. Los cursos para adultos mayores no pueden ser online, estos deben ser por otro canal, incluso radio.

18. los datos históricos de los ciudadanos a los cuales ya se tiene uso y están en manos de privados fueron tomados previo a la aparición de la regulación, si no se puede prohibir

su uso al menos se deberá informar a los ciudadanos de que esos datos ya se han vulnerado (por ejemplo la publicación de los datos del registro electoral u otras fuentes que se hicieron pública)

19. Más propaganda en los medios para que todos puedan acceder a información sobre ciberseguridad

20. Multas por mal uso.

21. Protección contra: grooming, "lenguaje inclusivo", doctrinas de identidad de género, etc.

22. Superintendencia de protección de datos ciudadanos y derecho a la conexión

23. Una propuesta para garantizar la privacidad y seguridad de los datos personales sería la creación de una identidad digital única y descentralizada basada en la tecnología blockchain y regulada por entidades gubernamentales competentes. Esta identidad digital permitiría a los usuarios tener un control total sobre su información personal, incluyendo la autorización de acceso a cualquier empresa o servicio que necesite utilizar dichos datos. Además, la tecnología blockchain aseguraría la transparencia y la integridad de la información, evitando cualquier intento de manipulación o uso indebido de los datos. Este enfoque se basaría en el concepto de PRIVACIDAD como prioridad, asegurando que los usuarios tengan control total sobre su información personal y que solo la compartan con las empresas y servicios que deseen. Esto permitiría una mayor confianza y seguridad en la gestión de datos personales, ya que los usuarios tendrían el control absoluto sobre su información y podrían garantizar que su privacidad sea respetada. En resumen, la creación de una identidad digital única y descentralizada soportada en blockchain y regulada, que permita el control de autorización y acceso a cualquier empresa o servicio que necesite utilizar datos personales, priorizando en el concepto de privacidad, sería una medida clave para garantizar la seguridad y privacidad de los datos personales.

Anexo 7: Respuestas adicionales en la pregunta M4

La pregunta M4 presentaba una serie de medidas propuestas, que podrían ser incluidas en la Política, en un objetivo central específico. El texto de la pregunta fue el siguiente: "*Por favor escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Coordinación nacional e internacional"*." La pregunta incluyó un comentario abierto donde las personas podían proponer

nuevas medidas; la lista a continuación detalla las medidas propuestas por las personas.

Las siguientes respuestas se presentan **sin editar** ni filtrar y ordenadas alfabéticamente:

1. Además de fortalecer Csirt se debe crear el Instituto Nacional de Ciberesilencia y Riesgo Tecnológico algo parecido a INDECI en España
2. Capacitación están al deve
3. Creación de cursos gratuito s para discapacitados
4. Creación de la Agencia Nacional e Ciberseguridad
5. Crear Centros de Respuesta a Incidentes Sectoriales (Ejemplo, Energía, Salud, Telecom)
6. Crear espacios de colaboración interna de la industria, como foros de operadores.
7. Crear superintendencia de protección de datos cuidamos
8. El poder judicial, la corte suprema, la fiscalía, así como las fuerzas de seguridad pública y de investigaciones deben especializarse en comprensión y lectura de información evacuada desde las plataformas digitales para limitar acciones de grupos o bots que evacuan información falsa.
9. En la actualidad las instituciones públicas asumen que delegar en un Datacenter externo (AWS u otros) es una solución tecnológica óptima, sin embargo, no tienen conciencia de la necesidad de autonomía y soberanía de los datos. Si en un momento no hay enlaces intermacionales u otro país establece restricciones por conflictos bélicos, las instituciones de Chile dejarían de operar. Se requiere tomar conciencia sobre la soberanía de los datos y de asegurar el funcionamiento de las instituciones nacionales. (Así como no se puede depender de un Registro Civil operado en China, tampoco es razonable depender de países Europeos o USA.)
10. Establecer instancias de cooperación con países avanzados en materia de respuesta de incidentes, como China; y ser anfitrión de eventos internacionales de ciberseguridad con invitados de estos países.
11. Fortalecer la dotacion de personal compentente en ciberseguridad del ministerio del interior, que sabe lo que hace y dice, no una agencia nueva que no tiene conocimiento y entorpecera las acciones

12. Fortalecer la investigación en centros nacionales (existe muy buena materia gris criolla)

13. Fortaleces no con contratar mas personas, se deben contratar personas capacitadas, expertos en ciberseguridad..

14. Generar proyectos de estandarización de infraestructura TI

15. Generar una sinergia y trabajo colaborativo entre universidades y fuerzas armadas... donde el objetivo sea la modernización de estado en todas sus aristas

16. Homologar los cursos de ciberseguridad que se impartan en pre grado y post grado e incentivar la creación de cursos en los colegios, los cuales deberían ser impartidos por la misma entidad gubernamental, que permitan no solo conocer sobre ciberseguridad, sino dedicarse a estos temas

17. Impulsar programas de financiamiento o becas para profesionales técnicos en Chile en la USACH, nuestro nivel de ciberseguridad es alto.

18. Impulsar programas de financiamiento o becas para profesionales técnicos en otros países más avanzados en ciberseguridad, pero no por parte del Conicyt, ya que van los mismos de siempre y no es una entidad confiable.

19. Incentivar a los centros educativos universitarios a realizar investigación en las áreas de análisis de entornos digitales gubernamentales, que permitan la detección oportuna de eventos que puedan gatillar en futuros incidentes de ciberseguridad.

20. Incorporar un csirt, noc y soc por repartición crítica del estado q actúen coordinadamente generando conocimiento y transferir solo a las reparticiones no críticas

21. ISRAEL!!

22. iumpulsar medidas efectivas pero con presupuesto para que los organismo publicos solucionen sus problemas

23. Mejorar internet y enseñar a traducir el ingles técnico en ésta area

24. No mas censura en Internet ni en los medios de comunicación por parte del estado o de los hackers contratados por agrupaciones ligadas a los ministros y al estado

25. También existen profesionales con experiencia y conocimientos a nivel nacional. Pero no están en el sector público porque no hay incentivos.

26. Tener una agencia de ciberseguridad al nivel de países desarrollados

27. Terminar con el nepotismo y cuoteo político de Boric
28. un organismo (no estatal) que coordine en forma eficiente y eficaz la información de gestión de la ciberseguridad entre empresas y particulares. integrada por ONG por ejemplo
29. Universidades públicas tomen rol activo

Anexo 8: Respuestas adicionales en la pregunta M5

La pregunta M5 presentaba una serie de medidas propuestas, que podrían ser incluidas en la Política, en un objetivo central específico. El texto de la pregunta fue el siguiente: "*Por favor escoge a lo más 3 medidas que creas que deben ser implementadas, en relación con el objetivo "Fomento a la industria de ciberseguridad"*." La pregunta incluyó un comentario abierto donde las personas podían proponer nuevas medidas; la lista a continuación detalla las medidas propuestas por las personas.

Las siguientes respuestas se presentan **sin editar** ni filtrar y ordenadas alfabéticamente:

1. Beneficios a empresas que fortalezcan estructuras internas en ámbitos de ciberseguridad. (inversion, foco)
2. Concientizar y educar desde edad temprana, para fomentar cultura de ciberseguridad
3. considerar un presupuesto para detectar y mitigar vulnerabilidades en sitios web de PYMES. (a nivel municipal, por ejemplo)
4. Creación de semillero especializado en ciberseguridad
5. Crear superintendencia de Ciber seguridad y protección de datos ciudadanos
6. Cumplir las promesas del Señor Presidente Boric como dar el 10% de ahorros de afp aumentar la pgu que dejó lista piñera y dejar de censurar en los medios
7. Desarrollar educación básica, media, pre grado y pos grado en Ciber seguridad.

8. Desarrollar una industria nacional y estatal para no depender de inversiones privadas

9. Disminuir impuestos y regulación

10. El Estado de Chile debe contar con infraestructura resilente y autónoma que asegure el funcionamiento del país en caso de una catástrofe o un conflicto bélico. Esto pasa por entender el tema de la autonomía funcional y soberanía de los datos como un desafío de seguridad nacional. Por tanto, se sugiere la creación de una infraestructura propia y autónoma que asegure el resguardo de los datos y servicios primarios. Por ejemplo, nic.cl mantiene servicios autónomos de DNS que aseguran el funcionamiento bajo dominios.cl, del mismo modo se debe asegurar que servicios patrimoniales como la Biblioteca Nacional, el Archivo Nacional sean debidamente digitalizados y respaldados, puesto que un incendio o un atentado pueden borrar de un plumazo todo nuestro patrimonio cultural e histórico.

11. Eliminar el IVA a los Servicios Profesionales de Ciberseguridad y Resilencia Tecnologica

12. Empresa Estatal de Ciberseguridad

13. En Chile NO deberia permitirse a otros paises inmiscuirse en nuestra red de seguridad, al ladron no le debo dejar las llaves de mi casa. Se pueden potenciar empresas locales, de esa manera no es necesario financiarlos, SI FUERA EN CHILE APOYO, de otra manera nada. Los que deseen venir a Chile con sus inversiones de seguridad, es bueno, pero por qué tenemos que darles incentivos.?, mejor financió lo que existe en el país, defendamos lo local. Por Favor.

14. En relación con el objetivo de "Fomento a la industria de ciberseguridad", algunas de las medidas que podrían ser consideradas son: Fomentar la educación y la formación de nuevos profesionales en el área de la ciberseguridad, incluyendo la creación de programas de capacitación y de intercambio de conocimientos entre los trabajadores y los estudiantes. Apoyar a las empresas y los profesionales que se dedican a la ciberseguridad, por ejemplo, a través de incentivos fiscales, financiamiento o la creación de espacios de colaboración y sinergia. Establecer regulaciones y normas claras para la protección de datos y la ciberseguridad, que permitan un marco legal sólido y seguro para el desarrollo de la industria.

15. Establecer convenios con Japon para cooperación e intercambio tecnologico

16. facilitar la posibilidad de traer tecnologías a Chile en forma rápida y expedita

17. Fomentar alianzas publico privadas para transferencia tecnológica que permita fortalecer la industria local

18. Fomentar en particular la generación de capacidad forense en ciberseguridad en Chile

19. Fomentar la enseñanza de ciencias básicas desde la temprana infancia, con adecuadas políticas de nutrición, y enseñanza de lectura y visión crítica de la sociedad. Gente malnutrida, no logra comprender conocimiento.

20. Fomentar y crear espacios para la utilización productiva de internet, para aprovechar la infraestructura, el desarrollo de capacidades tecnológicas y oportunidades laborales.para los

21. Fomento del Estado en el desarrollo del tema, a través de las unidades y subunidades ministeriales, Corfo y otras. Romper acuerdos comerciales que limitan la soberanía nacional en el tema y nos dejan a merced de las multinacionales.

22. Fortalecer desde la investigación la industria de la ciberseguridad, para que existan nuevos laboratorios o centros de investigación de ciberseguridad

23. Fortalecer la alianza público privada en la cual las universidades tengan un rol relevante

24. Fortalecer la demanda de ciberseguridad a través de un programa robusto de exisgencias normativas validadas a través del INN, en los SS.PP. y en los privados, a través de Chilecompra y los reguladores del mercado.

25. Generar incentivos para que las empresas adopten un standard mínimo de ciberseguridad

26. Generar un registro categorizado de las empresas locales y/o extranjeras con representación local, y de sus servicios, tal como el INCIBE español

27. impuesto 0(cero) a las empresas tecnologicas

28. Incentivos tributarios para fortalecer la propia infraestructura

29. Incorporar tecnología y conocimientos a la industria local (ellos sabrán si luego se internacionalizan)

30. Iniciativas de empresas con participación pública en estas materias, a través de CORFO, por ejemplo.

31. Inversión Estatal. Insisto, esto no se debe dejar en manos de privados.

32. Invertir en I+D+i nacional

33. La inversión debe ser para generar instancias de empresas locales u/o Carreras Técnicas en Universidades

34. Legislar

35. lo que hay fomentar es la Agencia Estatal de Ciberseguridad, de manera de evitar ser victimas de colusión industrial, que el estado no tenga el control nos hace dependientes y vulnerables.

36. No puedo optar por las alternativas ya que todos los dessarrollos a nivel nacional se crean sobre una plataforma base externa, lo que es una caja negra del punto de vista de seguridad.

37. Normar que las empresas/organizaciones, tengan un area que se haga cargo de la ciberseguridad, promoviendo que tengan personas y conocimiento para ello, mas alla de comprar herramientas que solo solucionan una parte del problema.

38. Obligatoriedad de contar con un especialista en prevención de ciberseguridad por empresa

39. plan semilla, lucas para que los especialistas sean capaces de independizar, ademas carreras de ciberseguridad, y los gerentes viejos saben de negocio pero no de ciberseguridad, los lideres del futuro si o si deben saber de ciberseguridad hoy en dia.

40. QUE NO SEAN EMPRESAS DE VIGILANCIA POR FAVOR

41. Ser país anfitrión con participación pública-privada en talleres, reuniones y charlas de transferencia de conocimientos y firma de acuerdos de cooperación y asesoría en ciberseguridad

42. Subsidio a emprendimientos tecnológicos al inicio del emprendimiento